IN THE SPECIFICATION:

Please amend paragraph [0013] as follows:

Described herein is a technique that will support multiple trusted provisioning domains (TPDs) for mobile devices and provide a solution to allow wireless carriers to control and distribute provisioning authorization without compromising security. As described in greater detail below, a primary TPD includes one or more provisioning servers that operate within a trusted environment on the wireless network and can provision the mobile devices. The primary TPD may distribute authorization to provision mobile devices to one or more secondary TPDs, each of which includes one or more provisioning servers ~~operates~~ that operate outside the trusted environment. Any of the secondary TPDs may operate on a network other than the wireless network. Digital signatures based on public key encryption can be used by any of the provisioning servers for increased security when provisioning the mobile devices.

Please amend paragraph [0032] as follows:

Figure 4 illustrates a process which may be performed by the browser 23 in the mobile device 1 in response to receiving ~~and~~ an MMC document. At block 401 the MMC module 24 in the browser 23 receives and parses the MMC document. At block 402 the MMC module 24 determines whether the source of the MMC document matches the object, browser:domain.trusted. If there is a match, then the process branches to block 405, in which the MMC module 24 causes the mobile device 1 to store the parameters (MMC objects) specified by the MMC document. At block 406 (or

block 310 in Figure 3) the browser 23 returns the completion result to the link server 4. If no match is found at block 402, the MMC module 24 determines at block 403 whether the source of the MMC document matches any browser:domain..<p>.trusted value previously provisioned in the mobile device 1.